面向系统确保的属性可计算方法

郭云川，殷丽华，刘礼才

摘要：由于系统运行环境的复杂化、用户的多样性以及软件正确性的不可判定，确保系统完全按照预期提供服务非常困难，因此安全评估方法与建模技术就成为系统确保研究中的重要内容和关键支撑技术，被用来尝试解决现有评估方法存在的局部性和状态爆炸以及对互联网的内容访问控制评估方法的缺失等问题。本文首先概述安全评估的相关工作，然后介绍我们的研究工作–信息内容安全的控制模型和定量评价方法以及混杂检测中的机密性与完整性模型。

关键词：系统确保；属性计算模型；定量评估；安全属性

1　引言

研究者对安全的认识经历了"从信息安全（IS）到信息确保（IA），从信息确保到软件确保（SwA），从软件确保到系统确保（SysA）"这样一个过程。从信息安全到信息确保，表明信息安全的研究是从技术走向服务，从提供技术手段走向提供安全服务能力。从信息确保到软件确保，表明信息安全的工作是从外部走向内部，从事后的补充性手段走向事前的防御性手段，在源头进行堵截。从软件确保到系统确保表明信息安全的工作是从局部走向整体，从单方面的关注安全到全局的考虑。

本质上，系统确保是确保硬软件系统在一定的环境下与用户交互过程中提供预期服务，并提供一种合理的确信级别。由于系统运行环境的复杂性、用户的多样性以及软件正确性的不可判定性，要确保系统绝对地按照预期服务是非常困难的。在这种情况下，对系统的评价显得至关重要。

近年来，针对安全分析与评估，研究人员提出了多种模型和方法。目前广泛使用的方法包括：基于规则的评估和基于模型的评估等。基于规则的评估从已知的安全问题中抽取特征，并归纳成规则表达式，将目标系统与已有的规则进行匹配，通过这种方法来寻找目标系统中存在的安全隐患。而基于模型的评估方法则是为整个系统建立模型，并通过模型获得系统所有可能的行为和状态，从而利用模型分析工具对系统整体的安全性进行评估。但这些方法均为通用的方法。通用方法的缺点在于可能偏离用户的安全需求，缺乏准确性。如，假设某个系统仅需要保障完整性，且该系统不存在不满足完整性的漏洞，但存在不满足其它安全性质的漏洞，此时，若采取通用的方法进行分析，由于通用的方法会分析系统所有的漏洞，这使得对系统的评价会偏离用户的关注点，影响评价结果的准确性。在这种情况下，修复对用户来说并不关心的漏洞会付出不必要的代价。

我们认为，系统确保所提供服务的落脚点又可以归结为信息或者系统组件的机密性、可鉴别性、可控性和可用性等安全属性的逻辑组合。因此，对系统及其各个组件所提供的安全服务进行安全度量就可以直接归结为对安全服务所依赖的安全属性的计算问题。

因此，我们选定"面向系统确保的安全属性计算模型与评估方法"作为课题研究和实现的突破口，在分析国内外安全属性和评估相关的模型、理论与技术的发展前沿和最新动态的基础上，借鉴属性分析和安全评估方向的已有成果，面向系统确保的实际需求，开展基于安全属性概率计算的评估模型、方法与技术的研究，增加对信息内容安全和网络访问控制的安

全评估能力。具体而言，属性可计算框架是从安全属性的角度出发，对系统提供的安全服务进行划分，研究子系统的层次关系，区分子服务之间的拓扑关系，评估子系统提供子服务的能力，通过概率传递，进而计算出各层次保障不同安全属性的能力。

同通用的评估方法相比，属性可计算框架不仅对具体的安全服务进行定量的评估，可有效克服通用评估方法的不准确，而且还能提供从不同角度（安全层次和安全要素）的求精功能，可对系统的不同层面进行评估，并发现已有技术的不足。同定性分析相比，属性可计算框架的长处在于：（1）更能发现保障安全需求的瓶颈，进而提高保障能力；（2）度量更为合理——定性分析结果往往是系统安全与不安全，而实际上要保持系统的绝对安全是不可能的，只要使对安全的破坏度保持在容许的范围内即可，而属性计算正是计算安全的度，这使得属性可计算框架更符合实际需求。同其它的量化分析相比，属性可计算框架是从系统提供不可分割的子服务的能力出发进行考察，能有效地减少主观赋值而导致的不客观性。

2 相关研究概述

为了实现基于属性可计算的思想对系统进行评估，首先要建立安全模型，分析属性之间的关系，然后以此为基础进行量化评估。为此，需要对安全属性的形式化描述。因此，下面从安全属性的形式化描述方法及关联性分析、安全模型及其量化分析方法来概述相关工作。

2.1 安全属性的形式化描述和关联性分析

安全属性的形式描述始于雅各布（J. Jacob）[1]，包括了两条主线：基于进程代数的方法和基于认知逻辑的方法。其中，基于进程代数对安全属性的研究也包括两个分支：基于进程代数的信息流的安全属性分析和基于进程代数的通用安全属性的分析。

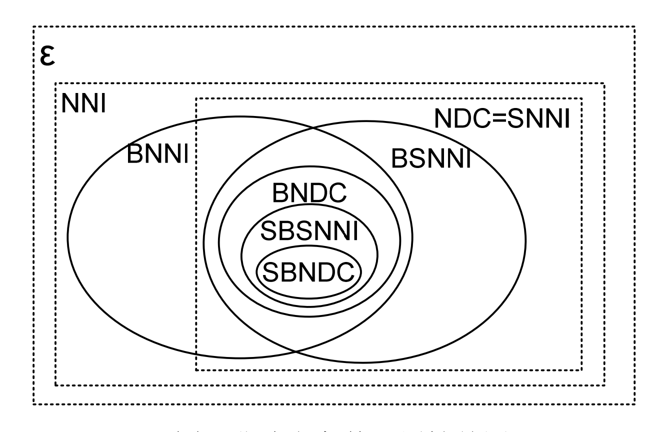


图1. 非确定条件下属性关图

基于进程代数的信息流的安全属性分析，主要研究如何利用进程代数来分析系统是否存在干扰，以及量化

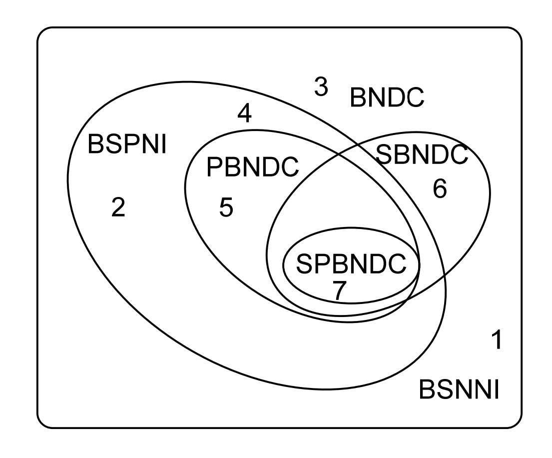


图2. 概率条件下的属性关系图

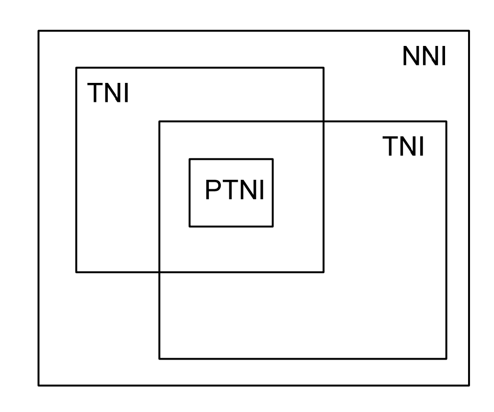


图3. 时间条件下的属性关系图

干扰中的信息泄漏情况。最早提出无干扰概念的是美国加利福利亚大学的戈恩（J. Goguen）[2, 3]，分析信息流中安全属性的代表性人物有意大利威尼斯东方大学（Università Ca' Foscari di Venezia）的福卡尔迪（R. Focardi）[4, 5]，意大利乌尔比诺大学（Università Degli Studi di Urbino Carlo Bo）的阿尔迪尼（A. Aldini）[6, 7]等。他们主要基于无干扰（Non- interference）的方法分析什么情况下存在信息泄露。总体思路是：首先设计合适的描述体系，而后分析信息流在什么类型情况下不存在信息泄露（不存在泄漏，则称之为一种属性），进而比较不同情况属性之间的关系。图 1、图 2 和图 3 分别给出了非确定条件下、概率条件下和时间概率条件下属性的文氏图[4,6,57]。图 1～3 中：NNI—Non-deterministic Non Interference（非确定无干扰），NDC—Non Deducibility on Compositions（组合上不可推演），BNNI—Bisimulation NNI（互模拟 NNI）, SNNI—Strong NNI（强 NNI），BSNNI-Bisimultion Strong NNI（互模拟强 NNI），BNDC—Bisimulation NDC（互模拟 NDC），SBSNN—Strong BSNNI（强 BSNNI），SBNDC—Strong BNDC（强 BNDC），BSPNI—Strong Bisimulation Probabilistic Non Interference（强互模拟概率无干扰），PBNDC—Probabilistic BNDC（概率 BNDC），SPSNDC—Strong PBNDC（强 PBNDC），TNI—Time Non Interference（时间无干扰），PTNI—Probabilistic TNI（概率 TNI）基于无干扰的安全分析。虽然以上很多工作都冠以“Security Properties（安全属性）”，但均只讨论信息的隐式泄漏情况，其实质是分析保密性，显然保密性只是安全属性的一部分。

基于进程代数的通用安全属性的分析方面，具有代表性的一项是英国伦敦大学 S. 施奈德（S. Schneider）的工作[8]，他利用通信顺序进程（CSP， Communicating Sequential Processes）来刻画和分析安全属性。安全属性的刻画独立于系统（安全协议），其刻画的属性包括机密性和基于消息的鉴别性（Message Authentication）。另一项是福卡尔迪[9, 10]的工作，他将系统的攻击看作一种干扰动作，进而基于迹(trace)描述一致性(Agreement property)、面向消息的可鉴别性(Message-Oriented Authentication)和不可否认性。得出的结论是：当且仅当系统在攻击存在情况的迹是系统不存在攻击的情况的迹前缀，系统满足这些安全属性。该工作很好地将无干扰的概念和通用的安全属性结合起来。然而，这些方式只分析了机密性、认证性和不可否认性。

英国剑桥大学的布罗斯（M. Burrows）等人采用认知逻辑来描述安全属性，做出了开创性的工作[11]，其目标是分析安全协议，该逻辑被称为 BAN 逻辑。BAN 逻辑的出现引发了大量分析安全协议认知逻辑的产生，比如 GNY 逻辑[12]、AT 逻辑[13]和 VO 逻辑[14]等。认知逻辑以诸如“主体知道…”、“主体相信…”的方式来表示知识（Knowledge）和“信仰”（Belief）。这种方式简单直观，使用灵活。然而，目前的认知逻辑方法并不能真正解决协议安全性分析中的问题，只能作为一个辅助手段来发现协议的安全漏洞。因为，许多认知逻辑化方法“证明”为安全的协议，后来发现仍是不安全的。其根本原因是这些认知逻辑缺乏明确的形式语义、解释存在歧义、公理不是概率真，逻辑规则可能不可靠[15]。

除了进程代数和认知逻辑之外，还有其它工作，比如文献[16, 17]。居根斯（S. Gürgens）[16]也将系统属性描述为动作迹，刻画了认证性和保密性，但这种方法非常不直观，很难推理属性之间的关系。在安全协议领域，还有很多方法来描述安全性质，比如徐蔚文所采用的线性时态逻辑[18]，潘廷（M. Panti ）所采用的计算树逻辑[19]等。另外美国 IBM 公司的阿尔帕恩和康奈尔大学的 F. 施奈德（B. Alpern F. Schneider）还给出了 Safety（保险性）和 Liveness（活性）[1]的形式描述，指出了每个属性都是 Safety 和 Liveness 的交集[20]，克拉克森（M. R. Clarkson）和 F.施奈德于 2008 年提出了超属性(HyperProperty)的概念[21] 。

2.2 基于属性的安全模型

[1] 直观地解释，在计算机安全领域，“Safety”是指坏事情不发生，“Liveness”是指好事情会发生

最早的机密性模型是 BLP 模型[22]，最早的完整性模型是 Biba 模型[23]。这两种模型的核心分别是“上写下读”和“上读下写”，在策略上是相反的。BLP 模型和 Biba 模型在研究界得到热烈的讨论，在工程中得到广泛的应用。除了这两种模型外，其它的模型包括 RBAC 模型、信息流模型、无干扰模型[2]、DTE 模型[24]、克拉克-威尔逊（Clark-Wilson）模型[25]、中国墙模型和 UCON 模型[26]等。这些模型各有千秋，如 RBAC 的结构简单，易于实现，也易与其他模型结合，但很难控制同一用户以不同的身份进入系统破坏安全性；信息流模型可以解决隐通道问题，但有些严格的安全条件是不可判定；中国墙模型同时涉及到保密性和完整性，其目的是为了解决商业中的利益冲突，在金融领域中有出色的表现；克拉克-威尔逊模型可以在理论上较好地解决完整性问题，但不易在现实系统中实现。纵观机密性和完整性模型，它们提供了在什么条件下是安全的，但不支持量化评估。

针对系统运行涉及的可用性、可靠性、生存性等属性的模型大部分基于图论和各种随机模型。S. 杰哈（Jha）等[52]将状态机模型、形式逻辑以及贝叶斯分析方法应用在对系统可用性和生存性的分析上。刘（Y. Liu）等[53]提供了可生存性评价的一般框架，假设系统失效时间满足随机分布，得到传输网络的马尔可夫模型，进而获得网络的生存性指标。这种基于排队论和可靠性理论的分析方法还被应用在自组织（ad-hoc）网络中[54]。J. 麦克德莫特（McDermott）等[55]使用随机进程代数（Stochastic Process Algebra）描述攻击者和系统的行为，并对系统的可用性和生存性进行了定量评价。M. 达西尔（Dacier）等[56]使用随机 Petri 网 SPN（Stochastic Petri Nets）分析系统安全性，将原子攻击转化为 SPN 中的随机变迁，通过求解 SPN 模型得到连续时间的马尔可夫链。高级随机模型有很强的描述能力，能够有效描述系统资源、服务等在系统运行中的情况，对系统的安全设计有很重要的意义，但用于系统安全性的量化分析容易产生状态爆炸问题。

2.3 安全属性量化评价方面

针对信息的机密性，有一些工作立足于从干扰的角度来度量信息的隐式泄露。最早机密性的量化工作可追溯到1982年，当时丹宁（D. Denning ）[28]给出了检测程序中信息泄露的方法。继丹宁之后，研究者进行了大量的工作。具有代表性的是： 1987年米伦（J. Millen）[29]首次研究了无干扰与互信息的一致关系，给出了信息流中的状态机模型与香农熵之间的关系。麦克林（J. McLean）[30]和格瑞（J. W. Gray III）[31] 等区分了非确定信息流和概率信息流，给出了概率信息流的通用模型。但丹宁和米伦方式的缺点在于其度量并不准确[32]，麦克林工作的缺点是很难区分高低安全级对象之间的因果关系。另外，这些工作都是基于香农熵的，然而，2009年史密斯（G. Smith） [33]指出即使某个变量很容易被猜测到，它也可能具有任意大的香农熵。这导致基于香农熵的方式并不一定准确。史密斯进而以贝叶斯风险为基础，利用雷尼（Rényi）最小熵来度量不确定性，以此给出信息泄露的度量方法。2005年克拉克森 [34]利用概率分布来为攻击者的“信仰”建模，而后利用贝叶斯技术来修正该信仰，进而利用相对熵来量化基于“信仰”的信息流。2010年哈马度（S. Hamadou）[35]认为基于“信仰”和贝叶斯风险方式量化信息流也是不准确的，进而提出了一种混合指标评价。2008年阿迪尼（A. Aldini）等 [36-38]采用概率弱互模拟来标识信息的泄露，而后利用不同进程中相同的动作的最大概率差来度量信息的泄露。然而，我们的实验表明：这种度量方式并不准确[39]。在抽象解释层面，安冈（H. Yasuoka） [40]分析了基于熵方式进行量化分析的难度和可能性，指出对于任意的***k***，现有的方式都不是k安全（***k-safety***），因此不能采用自组合方式来量化信息泄露。库孚（Kǒpf） [41]利用猜测（guessed）熵给出了边界信道攻击的度量，并依据程序执行的次数来量化其信息泄露界。

上面的分析表明：虽然目前对信息流的量化作了深入研究，但是如何保障量化的准确性仍是一个难题；另外，也少有工作分析信息泄露量的上下界；更重要的是大多数对信息流的

度量研究聚焦于信息的泄漏，很少研究信息流的完整性。2010 年克拉克森开启了面向信息流完整性的量化评估[42]，他以互信息为基础，区分污染点和抑制点，给出了完整性破坏度的计算方法。虽然克拉克森首先开启了面向信息流完整性的量化评价，但其度量方式及评价指标都比较单一，没有考虑拓扑变化、污点及抑制点可能传播的情况，也没有考虑势差等对完整性的影响。因此，其应用范围有限。

由利特尔伍德（B. Littlewood）提出来的概率定量衡量安全属性的方法[43] 针对系统运行的安全性以及服务的可用性，试图找出可信赖评价与安全属性评价的相似之处，然后利用可信赖评估的思想给出可用性、可靠性、生存性等安全属性的指标型概率定义。然而可信赖分析认为系统失效是由于组件随机故障引起的，而实际的网络与信息系统中的安全故障是由恶意攻击而引起的“拜占庭（Byzantine）”式故障，因而在可信赖评估与安全属性定量评估之间造成了一道鸿沟。而基于图论、排队论和随机模型的定量分析方法[44]则由于目前网络系统的规模大、结构复杂而出现状态爆炸问题，只能针对局部网络或小规模系统进行，没有形成系统的实用化的评价方法和实现机制，且存在安全属性的内涵不一致和重叠的问题。

3 研究进展

面向系统确保的属性可计算实际上要研究可控性、可用性、可鉴别性及机密性等的计算模型。

3.1 互联网内容安全的控制模型 ICCON 及评价[2]

虽然访问控制和安全评价的理论与实践均得到重大发展，但目前信息内容安全的控制模型和定量评价方法少有研究。

3.1.1 引用监视器的作用位置

引用监视器存储访问控制策略和判定规则，并依据这些规则控制主体对客体的访问，是访问控制的核心组件。在信息内容安全中应用的监视器有三种：服务端引用监视器（SRM，Server-side Reference Monitor），客户端引用监视器（CRM, Client-side Reference Monitor）及网络引用监视器（NRM, Networked Reference Monitor），如图 4~6。服务端引用监视器在服务端检查从客体流向主体的信息流或者主体对客体进行的操作，客户端引用服务器在客户端检查从客体流向主体的信息流或者主体对客体进行的操作，网络引用监视器负责从网络端实施内容安全的控制过程。

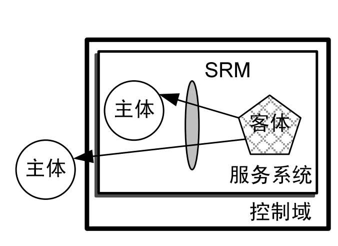
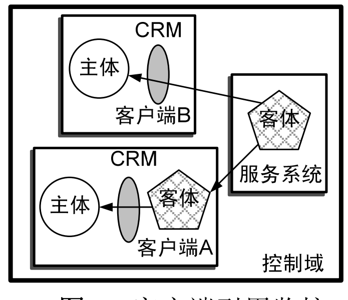
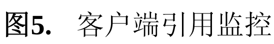


图4. 服务端引用监控




图5. 客户端引用监控

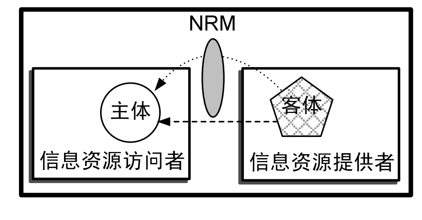


图6. 网络引用监控

3.1.2 控制模型

有害信息的传播者不可能主动将信息提交给网络引用监视器进行分析，因此为了对内容

---

[2] 本小结主要引自方滨兴、郭云川、周渊《互联网信息内容安全的 ICCON 控制模型及评价》一文

进行控制，网络引用监视器必需先获取访问信息。由于获取的信息可能没有明确的属性标识，所以对获取的信息需要鉴别，最后需要对不合理的信息流动产生响应。因此，网络引用监视器中控制过程包括三个阶段：信息获取，信息鉴别和响应。“谁与谁在通信”，“以什么方式通信”和“通信的内容是什么”构成了通信的三个基本要素，因此控制过程的对象包括三个：身份、内容和行为。

基于信息内容安全的控制过程和作用对象，可以得到互联网信息内容控制的三种基本模型：基于内容的控制模型、基于身份的控制模型和基于行为的控制模型，分别称为 $ICCON_C$、$ICCON_I$ 和 $ICCON_B$，这三个模型的组合为 ICCON， 如图 7。

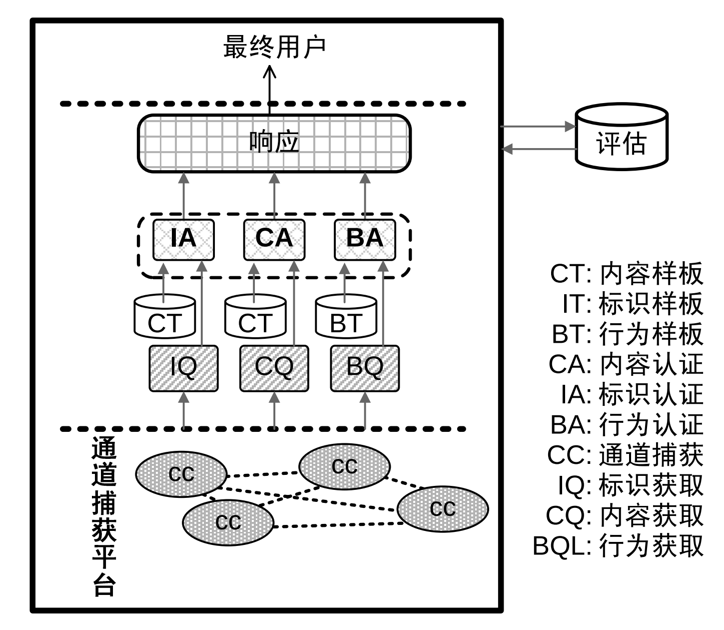


图7. 内容安全控制框架

3.1.3 评价方法

评价信息内容安全的控制能力是信息内容安全研究的一个重点。目前关注的评价方法有两种：社会评价和技术评价。社会评价是从社会需求出发，完全针对信息内容，评价其实施控制效果，体现对内容安全的控制结果与社会预期的差别；技术评价是针对某种具体的控制手段来评价其控制效果，反映在给定条件下，被评价技术实现的结果和该技术的预期结果的差别。

对每个评价常采用两个指标：漏控率和误控率。漏控率是指预期应对信息的流动进行响应而未响应的概率，误控率则是指预期不应响应而响应的概率。这里的预期可能是从社会角度的预期，也可能是从技术角度的预期。这样评价指标包含了四类：社会评价漏控率、社会评价误控率、技术评价漏控率和技术评价误控率。本文主要关注技术评价，为此，我们将对信息内容安全控制能力的评价转为对控制过程的评价，即评价信息获取能力、鉴别能力和响应能力，最终获得对信息内容安全控制能力的评价。

3.2 混杂检测中的机密性与完整性模型

移动计算中的机密性和完整性是计算机安全模型的重要核心问题之一。为了保障移动计算中的机密性和完整性，需要相应的控制模型。最早的机密性模型是 BLP 模型，最早的完整性模型是 Biba 模型，这两种模型在流向上是矛盾的。由于它们信息流方向相反，如何合成这两种模型需要深入研究。文献[45]指出，有可能把完整性和机密性的存取类进行合并，从而复合 BLP 和 Biba 模型；文献[46]指出 BLP 模型和 Biba 模型均属于基于格的信息流模型，因此，可利用“格的直积仍为格”这种性质将这两种模型进行复合。然而，基于格的直积方式不能处理流向之间的矛盾性；文献[47, 48, 49]基于可信主体提出了一种新的安全模型，复合了 BLP 模型和 Biba 模型，但这个可信主体的权限过大可能会破坏系统安全性；文献[50]将访问信息的主体划分为四类：直接创建者和直接读者，间接创建者和间接读者，并通过“读”来保障程序的机密性，通过“写”来保障程序的完整性。但是，“读”和“写”这两个操作均与机密性模型和完整性模型密切相关，仅通过单个的“读”或“写”操作能否有效地保障机密性或完整性，这需要进一步研究；文献[51]在降级策略及程序等价的环境下给出统一的机

密性和完整性策略，但并未给出如何处理 BLP 模型和 Biba 模型在信息流上的矛盾性。

基于混杂类型检测的安全 π 演算（Hybrid Typed Security Pi, HTSPi）的思路是利用 π 演算能够有效为移动并发系统的特征建模，再借鉴程序语言中不同类型变量之间的赋值方式。该方法利用静态类型检测保障低机密级信息只能向同等或更高机密级信息流动，高完整级信息向同等或更低完整级信息流动，针对 BLP 模型和 Biba 模型信息流向相反的特性，利用动态检测来进行调整。这一方法将静态检测和动态检测有机地整合在一起，形成了一种统一的形式框架，既能保障机密性又能保障完整性，可高效静态地推理系统的行为。

4 小结

系统确保是为了保证硬软件系统在一定的环境下与用户交互过程中能提供预期服务。为了保障系统提供预期的服务，安全评估是极其重要的环节。在众多的安全评估方式中，安全属性可计算理论是一种重要的方式，可以从不同的抽象层面、不同的侧重角度对系统的安全性能进行评估。然而目前这一方向的研究尚处于初始阶段，我们期望能引起更多研究者对该方法的重视，从安全属性的角度对系统的安全评估进行深入的研究。

参考文献：

[1] J. Jeremy. *Security Specifications*. Proceedings of the IEEE Symposium on Security and Privacy. 1988, 14-23

[2] J. A. Goguen, J. Meseguer. *Security Policies and Security Models*. Proceedings of IEEE Symposium on Security and Privacy. 1982, 11-20

[3] J. A. Goguen J. Meseguer. *Inference Control and Unwinding*. Proceedings of IEEE Symposium on Security and Privacy. 1984,75-86

[4] R. Focardi, R. Gorrieri. *Classification of Security Properties (Part I: Information Flow)*. Proceedings of Foundations of Security Analysis and Design. LNCS 2171. 2001

[5] R. Focardi, R. Gorrieri and F. Martinelli. *Classification of Security Properties (Part II: Network Security)*. Proceedings of Foundations of Security Analysis and Design II. LNCS 2946. 2004

[6] A. Aldini, M. Bravetti and R. Gorrieri. *A Process-Algebraic Approach for the Analysis of Probabilistic Non-Interference*. *Journal of Computer Security.* 2004, 12(2):191-245

[7] A. Aldini. *Classification of Security Properties in a Linda-Like Process Algebra*. Journal of Science of Computer Programming, Special Issue on Security Issues in Coordination Models, Languages and Systems. 2006,63(1):16-38

[8] S. Schneider. *Security Properties and CSP*. Proceedings of IEEE Symposium on Security and Privacy. 1996,174-187

[9] R. Focardi, F. Martinelli. *A Uniform Approach for the Definition of Security Properties*. Proceedings of Proceedings of the World Congress on Formal Methods in the Development of Computing Systems, LNCS 1708. 1999,794 - 813

[10] R. Focardi, R. Gorrieri and F. Martinelli. *A Comparison of Three Authentication Properties*. *Theoretical Computer Science.* 2003,291(3):285 - 327

[11] M. Burrows, M. Abadi and R. M. Needham. *A Logic of Authentication*. ACM Transactions on Computer Systems. 1990, 8(1):18-36

[12] L. Gong, R. Needham and R. Yahalom. *Reasoning About Belief in Cryptographic Protocols*. Proceedings of Proceedings of the IEEE Symposium on Research in Security and Privacy. 1990,234-248

[13] M. Abadi, M. R. Tuttle. *A Semantics for a Logic of Authentication.* Proceedings of Annual ACM Symposium on Principles of Distributed Computing. 1991,201 – 216

[14] PC. Van Oorschot. *Extending Cryptographic Logics of Belief to Key Agreement Protocols*. Proceedings of the ACM conference on Computer and communications security. 1994,232 – 243

[15] 李益发. 密码协议安全性分析中的逻辑化方法——一种新的 ban 类逻辑. 解放军信息工程大学, 2001

[16] Sigrid Gürgens, Peter Ochsenschläger and Carsten Rudolph. *On a Formal Framework for Security Properties*. Computer Standards & Interfaces. 2005,27(5):457-466

[17] A. Mana, G. Pujol, *Towards Formal Specification of Abstract Security Properties.* Proceedings of the Third International Conference on Availability, Reliability and Security 2008,80-87

[18] 陆鑫达, 徐蔚文. 身份认证协议的模型检测分析. 计算机学报. 2003, 26(2):195-201

[19] L. Spalazzi, M. Panti, S. Tacconi, *Using the Nusmv Model Checker to Verify the Kerberos Protocol*. Proceedings of Proceedings of the Collaborative Technologies Symposium 2002,230-236

[20] B. Alpern, F. B. Schneider. *Defining Liveness*. Information Processing Letters. 1985, 21(4):181-185

[21] M. Clarkson, F. Schneider. *Hyperproperties*. *Proceedings of Computer Security Foundations Symposium*. 2008,51-65

[22] D. E. Bell, L. J. Lapadula. *Secure Computer Systems: A Mathematical Model*. Hanscom AFB, Bedford, MA, Rep. FSD-TR- 73-278, vol. 1, ESD/AFSC. 1973

[23] K. J. Biba. *Integrity Considerations for Secure Computer System*. Technical Report ESD-TR-. 76-372, MTR-3153, The MITRE Corporation. 1977

[24] L. Badger, D. F. Sterne, D. L. Sherman, K. M. Walker, S. A. Haghighat. *A Domain and Type Enforcement Unix Prototype*. Proceedings of the Fifth USENIX UNIX Security Symposium. 1995,127-140

[25] D. D. Clark, D. R. Wilson. *A Comparison of Commercial and Military Computer Security Policies*. Proceedings of the IEEE Symposium on Security and Privacy. 1987, 184~194

[26] J. Park, R. Sandhu. *The UCONABC Usage Control Model.* ACM Transactions on Information and System Security. 2004, 7(1):128 -174

[27] J. K. Millen, *Finite-State Noiseless Covert Channels.* Proceedings of Proceedings of the Computer Security Foundations Workshop. 1989,81-86

[28] D. Denning, *Cryptography and Data Security.* Addison-Wesley Longman Publishing Co., Inc. Boston, MA, USA, 1982

[29] J. K. Millen, *Covert Channel Capacity.* Proceedings of IEEE Symposium on Research in Security and Privacy. 1987,60-66

[30] J. Mclean, *Security Models and Information Flow. Proceedings of IEEE Computer Society Symposium on Security and Privacy.* 1990, 180-187

[31] J. W. Gray III. *Toward a Mathematical Foundation for Information Flow Security. Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy.* 1991, 21-34

[32] D. Clark, S. Hunt, P. Malacaria. *A Static Analysis for Quantifying Information Flow in a Simple Imperative Language. Journal of Computer Security*，2007,15(3):321-371

[33] G. Smith. *On the Foundations of Quantitative Information Flow. Lecture Notes in Computer Science.* 2009,5504:288-302

[34] M. R. Clarkson, A. C. Myers, F. B. Schneider. *Belief in Information Flow. Proceedings of Computer Security Foundations,(CSF05)*. 2005,31-45

[35] S. Hamadou, V. Sassone, C. Palamidessi. *Reconciling Belief and Vulnerability in Information Flow. Proceedings of IEEE Symposium on Security and Privacy (SP).* 2010,79-92

[36] A. Aldini, D. Pierro. *A Quantitative Approach to Noninterference for Probabilistic Systems Electronic Notes in Theoretical Computer Science.* 2004, 99(6):155-182

[37] A. Aldini, D. Pierro. *Estimating the Maximum Information Leakage. International Journal of Information Security*. 2008, 7(3):219-242

[38] Pierro A D, Hankin C, Wiklicky H. *Approximate Non-Interference. Journal of Computer Security.* 2004, 12:37-82

[39] G. YunChuan, Y. Lihua, Z. Yuan, L. Chao, G. Li, *Simulation Analysis of Probability Timing Covert Channels.* Proceedings of IEEE International Conference on Networking, Architecture, and Storage (NAS 2009) 2009,325-332

[40] H. Yasuoka, Terauchi T. *Quantitative Information Flow-Verification Hardness and Possibilities.* Proceedings of IEEE Computer Security Foundations Symposium (CSF),. 2010,15-27

[41] B. Kǒpf, D. Basin. *An Information-Theoretic Model for Adaptive Side-Channel Attacks*. Proceedings of the 14th ACM conference on Computer and communications security 2007, 286-296

[42] M. R. Clarkson, F. B. Schneider. Quantification of Integrity. Proceedings of IEEE Symposium on Computer Security Foundations. 2010,28-43

[43] B. Littlewood, S. Brocklehurst, N. Fenton, P. Mellor, S. Page, D. Wright, J. Dobson, J. McDermid, D. Gollmann. *Towards Operational Measures of Computer Security.* Journal of Computer Security, 1993,2:211-229

[44] L. Lamport, R. Shostak, M. Pease. *The Byzantine Generals Problem*. ACM Transactions on Programming Languages and Systems. 1982, 4 (3):382-401

[45] M. Gasser. *Building a Secure Computer System*, 1988

[46] R. S. Sandhu. *Lattice-Based Access Control Models*. IEEE Computer. 1993, 26(11):9-19

[47] 郑志蓉, 蔡谊, 沈昌祥．基于多级安全策略的二维标识模型．计算机学报. 2004, 27(5):619-624

[48] 沈昌祥，李益发．一种新的操作系统安全模型．中国科学(E 辑,信息科学). 2006, 36(4):347~356

[49] 刘威鹏，张兴．基于非传递无干扰理论的二元多级安全模型研究．通信学报. 2009, 39(2):52-58

[50] N. Heintze, J. G. Riecke. *The Slam Calculus: Programming with Secrecy and Integrity*. Proceedings of the 25th ACM SIGPLAN-SIGACT symposium on Principles of programming languages. 1998, 365-377

[51] P. LI, S. Zdancewic. *Unifying Confidentiality and Integrity in Downgrading Policies*. Proceedings of the LICS'05 Affiliated Workshop on Foundations of Computer Security (FCS). 2005,45-54

[52] S. Jha, R. Linger, T. Longstaff, J. Wing. *Survivability Analysis of Network Specifications*. Dependable Systems and Networks, New York, USA, IEEE Press, 2000:613~622

[53] Y. Liu, K. S. Trivedi. *A General Framework for Network Survivability Quantification*. the 12th GI/ITG Conference Measuring, Modeling and Evaluation of Computer and Communication Systems, Dresden, Germany, 2004,369~378

[54] D. Chen, S. Garg, K. S. Trivedi. *Network Survivability Performance Evaluation: A Quantitative Approach with Applications in Wireless Ad-hoc Networks.* the 5th ACM International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems（MSWiM 2002）, Atlanta, 2002,61~68

[55] J. McDermott. *Attack-Potential-based Survivability Modeling for High-Consequence Systems.* the 3rd IEEE International Workshop on Infromation Assureance (IWIA'05), Callege Park, Maryland, USA, 2005,119~130

[56] M. Dacier, Y. Deswarte, M. Kaaniche. *Models and tools for quantitative assessment of operational security. Information systems security: facing the information society of the 21st century,* 1996, 177 - 186

[57] R. Lanotte, A. Schettini, A. Troina. *A Classification of Time and/or Probability Dependent Security Properties*. Electronic Notes in Theoretical Computer Science.2006, 153(177–193)

作者简介：

郭云川： 中国科学院计算技术研究所信息安全研究中心 博士研究生

殷丽华： 中国科学院计算技术研究所信息安全研究中心 博士后
yinlihua@software.ict.ac.cn

刘礼才： 中国科学院计算技术研究所信息安全研究中心 博士研究生